April 25, 2002

The Honorable Tommy G. Thompson
Secretary, U.S. Department of Health and Human Services
Office of Civil Rights
Attention: Privacy 2
Hubert H. Humphrey Building
Room 425 A
200 Independence Avenue, SW
Washington, DC 20201

Dear Secretary Thompson:

The University of California (University) welcomes the opportunity to provide comments to the Secretary's March 27, 2002 proposal (NPRM) to modify the federal medical Privacy Rule.

The University of California is one of the largest, if not the largest, health professions education system in the world and is world-renown for the excellence of the numerous training programs and the quality of the health professionals trained in a broad range of disciplines, including medicine, nursing, pharmacy, dentistry, public health, and optometry. On an annual basis, approximately 13,000 undergraduate and graduate students are enrolled in the health professions. The University's eight licensed acute care hospitals and two licensed psychiatric hospitals provide over 750,000 inpatient days of care to more than 130,000 patients, with 3.3 million outpatient visits per year. The 50,000 plus faculty and non-faculty employees of the University's five academic health centers are among the finest health sciences professionals in the world. They provide the core of excellence that is the heart of the University's education, research and teaching missions.

The University offers its strong endorsement of the Secretary's efforts to propose changes that will relieve the unintended negative effects and administrative burdens of the Privacy Rule and provide for increased "workability."

The purpose of the University's response is three-fold:

1) To provide, where appropriate, specific responses as requested by the Secretary in the NPRM;
2) To seek clarification regarding certain areas where we have difficulty in either determining the intent of the regulation or implementing the proposed change; and
3) To provide recommendations that will support the Secretary's intent to increase the workability of the Privacy Rule and mitigate the administrative burden.

A. Effective Date of Any Revisions and Education of the Workforce

Statutory requirements provide that any revisions must become effective by October 13, 2002.

Recommendation: The University urges the Secretary to finalize any revisions as soon as possible so that covered entities can proceed with their business plan in order to meet the compliance deadline. For example, expediting the effective date for revisions will enable covered entities to proceed with workforce education well in advance of April 2003.

Recommendation: Although not specifically addressed in the NPRM, the University is requesting that the Secretary clarify expectations regarding the education of faculty and trainees who function in multiple covered entities. In academic health centers, faculty and trainees carry out their responsibilities in a number of covered entities, both "parent" institution and affiliated covered entities. It would reduce administrative burden and, in particular, training costs, if the Secretary would clarify that an individual's participation in one HIPAA training program at the "parent" covered entity would meet the Privacy Rule education requirements.

B. Uses and Disclosures for Treatment, Payment and Operations

The University endorses the Secretary's proposed changes to: allow a covered entity to use or disclose PHI for its own treatment, payment or operations without consent or authorization; eliminate the transition provisions; and broaden the uses and disclosures between covered entities that are permitted as part of treatment, payment and health care operations. These changes should enhance access to care and address a number of the concerns expressed by health care providers.

1. Initial Moment and Good Faith Effort.

The practical problems of providing Notice and obtaining a written acknowledgement from a patient at the "initial moment" are the same as those a provider would encounter when obtaining a written consent. The University anticipates that we will experience additional administrative burdens because of the strengthened Notice requirements and expectations on the part of the Secretary and the patient that there will be sufficient opportunities at the time of the initial face-to-face patient contact to "engage in important discussions regarding the use and disclosure of their health information." This burden on health care providers will come at a time when a provider and patient's attention and concerns are focused on health care issues unrelated to privacy practices. These discussions occur at admission or registration and could involve covered entity employees unable to negotiate modifications to privacy rights. Further, the assumption is that the "initial moment" involves personal contact, but it may be through other means. Ambiguity remains as to the requirements of a "good faith effort" on the part of providers. Unfortunately, ambiguity could result in arbitrary determinations by federal auditors that a provider has violated the Privacy Rule.

Moreover, since only direct treatment providers, not other covered entities, are required to make this good faith effort, it places a disproportionate and additional administrative burden on those providers who are "on the front line" with patients.

Recommendation: To assist with effective implementation of the "good faith effort" provision and provide for an efficient admissions process so that the patient receives timely care, the

University recommends that a good faith effort would be comparable to what is currently done by admissions clerks and others at the time of admission when a patient receives the provider's Treatment Terms and Conditions and consents to treatment. A "good faith effort" should consist of: 1) written policies and practices that provide: "At the time of a patient's initial face-to-face contact with the University's health care provider, the University will provide the patient with a Notice of Privacy Practices and request a written acknowledgment, either by signature or initial, that the patient has received the Notice"; and 2) appropriate education of employees responsible for admitting patients. If the patient does not provide a written acknowledgement, a note stating: "The patient refused to provide a written acknowledgement of receipt of the Notice of Privacy Practices." would suffice for documentation purposes.

2. Emergency Treatment Situations

The University, which operates four Level 1 Trauma Centers and provides services to the fifth, endorses the Secretary's recognition that it is not practicable during emergency treatment situations to provide notice and obtain written acknowledgement until "reasonably practicable after the emergency treatment." Emergency Departments and Trauma Centers operated by the University serve not only the insured, but we also provide care to all who enter our doors, including the uninsured and Medicaid beneficiaries. The very nature of these types of emergency care centers make it very difficult to meet the "initial moment" expectations of the NPRM, and the NPRM does not clarify what activities qualify for the emergency treatment exception.

Recommendation: To ease the administrative burden and provide for timely and effective treatment, the University recommends that, in addition to other types of emergency services as determined by the individual provider, all care provided in Emergency Departments and Trauma Centers would be defined as "emergency treatment" for purposes of the exception.

3. Disclosure of PHI to Another Covered Entity

As an academic health center, the University appreciates the proposal to permit a covered entity to disclose PHI to another covered entity for health care operations, including training programs; however, the disclosure is limited to the extent that each entity has a relationship with the individual who is the subject of the information being requested. In an academic setting, there may be situations where trainees rotate to clinical settings (i.e., other covered entities) and then bring clinical care information back to the University's classroom or clinical setting as a part of their training requirements. However, the University may not have a direct treatment relationship to the patient.

Recommendation: Since the NPRM would allow covered entities participating in an OHCA to share PHI for the health care operations of the OHCA, regardless of the relationship with the patient, the University recommends that this principle be extended to those health care operations/training relationships between two covered entities and clarify the definition of relationship to include "a teaching relationship with the patient."

Finally, since the disclosure is to another covered entity for treatment, payment or operations, we assume that there would be no required accounting of those disclosures and would appreciate clarification of that conclusion.

B. Minimum Necessary and Incidental Uses and Disclosures

1. Incidental Uses and Disclosures

The University endorses the NPRM modifications which explicitly permit certain incidental uses and disclosures that occur as a result of an otherwise permitted use or disclosure and appreciates the Secretary's recognition that these communications are a part of providing health care. Both the July 6th Department guidance and the discussion of the March 27th NPRM affirm that the Privacy Rule is not intended to impede customary and necessary health care communications or practices, including incidental disclosures, so long as reasonable safeguards are employed. The University intends to develop policies and procedures that would demonstrate to a reasonable person that the University has applied appropriate and reasonable safeguards.

However, the NPRM discussion differs from that of the July 6th guidance in that it states: "the proposed modification is not intended to excuse erroneous uses or disclosures or those that result from mistake." While the University will make a concerted effort, including written policies, procedures and education, to prevent errors or mistakes, isolated mistakes will occur. The NPRM discussion suggests that even a single, unintentional incident or mistake could subject a covered entity to a determination it has violated the Privacy Rule.

Request for Clarification: The University requests a clarification of whether the Secretary intended for a single, isolated incident to be a violation of The Privacy Rule or rather the discussion was referencing those situations where there could be systemic errors or a pattern of reckless disregard.

2. Minimum Necessary Standard

In implementing the minimum necessary standard, the NPRM discussion notes: "Covered entities may, however, need to make certain adjustments to their facilities, as reasonable, to minimize access or provide additional security… For example, covered entities may decide to provide additional security, such as passwords, on computers that maintain PHI." In another section of the discussion, the NPRM states that "The Department agrees with the NCVHS about the need for further guidance on the minimum necessary standard and intends to...provide additional technical assistance materials to help covered entities implement the provisions."

Request for Clarification: The reference to implementation of security safeguards and technical assistance materials suggests that failure to provide technical and physical security for the minimum necessary standard could be a violation of the Privacy Rule, particularly in a paper medical record environment. The University agrees with the suggestion that physical and technical security is necessary to implementation of the Privacy Rule, as particularly exemplified in the minimum necessary standard, but the University has been awaiting finalization of the Security Rule prior to implementing physical and other safeguards.

The University requests clarification regarding the expectations of DHHS since this places an unnecessary administrative burden on covered entities. Moreover, the University urges DHHS to expedite the finalization of the Security Rule to minimize costs and maximize compliance with the Privacy Rule.

C. Business Associate Provisions

The University appreciates the Secretary's willingness to extend the time for compliance for adding the business associate language to our existing contracts. Covered entities, however, are still required to comply with HIPAA mandated responsibilities by April 2003. For example, a covered entity must make PHI held by a business associate available to the Secretary upon request and ensure that an individual may access or amend his/her PHI held by a business associate. These requirements will be difficult, if not impossible, to ensure without a business associate agreement. Therefore, the additional amount of time may not be of assistance to most covered entities.

Additionally, the Model Business Associate Contract provisions create an additional layer of confusion in the contracting process. The model language imposes duties on the covered entity that are not required in the Privacy Rule. For instance, the model language states that the covered entity shall provide the business associate with its notice of privacy practices and that the covered entity must provide the Business Associate with any changes, revocations, restrictions, etc. to the individual's permission to use or disclose PHI. Additionally we are puzzled by the inclusion of certain standard contract terms such as "term" and "termination" that are not required by the regulations, while other important standard terms such as "insurance" and "indemnification" that may have a significant impact on assuring compliance with HIPAA are excluded.

Moreover, the Model Business Associate Contract does not require compliance with the Electronic Transactions Standards by business associates if they are performing electronic transactions on behalf of the covered entity.

Recommendation: The Model Business Associate Contract should correspond to the specific requirements of the regulations or, alternatively, clearly identify those provisions that are optional. The University recommends that the Model Business Associate Contract be revised to only include language as required in The Privacy Rule.

Also, in those cases where the Business Associate Agreement does not go into effect until April 2004, the Privacy Rule should be modified so that the covered entity is exempted from complying with any patient requests for accounting, access to or amendment of PHI held by a business associate until the effective date of the Business Associate Agreement.

Again, if the Model Contract is designed to be the industry standard, it should be comprehensive and, therefore, reference the trading partner and require compliance with the electronic transactions. For example, "Business Associate shall comply with all applicable federal and state laws and regulations, including the standards for electronic transactions, 45 CFR Parts 160 & 162, on or before October 16 (2003 or 2004)."

D. Marketing

The University endorses the Secretary's effort to clarify the confusion regarding patient communications that are strictly marketing and those that are health care communications between provider and patient. Through those communications, many covered entities provide information about resources, educational opportunities, products, and services that may benefit the patient's overall health and well-being. The current definition of marketing may

inadvertently limit or prevent necessary or beneficial communications because the current exceptions would not allow those communications. For example, a new mother could benefit from a breast pump sold through a local drug store or breastfeeding classes provided in the community; patients with high cholesterol could benefit from new drugs or a cooking class.

Recommendation: The University recommends that the following two exceptions be included in the list of three exceptions to marketing:

1) to describe the entities participating in a health care provider network or health plan network, or to describe if, and the extent to which, a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits;
2) for treatment of that individual;
3) for case management or care coordination for that individual, or to direct or recommend alternative treatments, health care providers, or setting of care to that individual;
4) communications, either written or oral, between a physician and patient regarding products or services that may be of benefit or interest to the patient; and
5) communications, either written or oral, between a covered entity and patient regarding products or services that may be of benefit or interest to the patient and relate to the patient's present condition and/or treatment.

E. Fundraising

1. Fundraising by the covered entity

The majority of an academic health center's fund raising comes from individual philanthropists and, in particular, grateful patients. The rules requiring authorization or creating exceptions to the authorization requirements allow limited information for fund raising purposes to be given to Business Associates or a related foundation, while placing no such limits on the covered entity. The University reads 45 CFR 164.514 (f)(1) to permit the University's covered entity or health care component to use PHI for fund raising without authorization and has interpreted the current Privacy Rule to mean that the University's covered entity may engage in fundraising activities with its patients without an authorization so long as: 1) any PHI used for those health care operations/fundraising purposes are not used or disclosed outside of the University's health care component; 2) the patient is notified of fundraising in the Notice of Privacy Practices; and 3) the patient receives a description of how she may opt out of receiving any further fundraising communications.

Request for Confirmation or Recommendation: The University requests that the Secretary confirm the University's interpretation of The Privacy Rule's standards for fundraising when it is carried out by a covered entity. If the University's interpretation is incorrect, then the University recommends that an amendment be drafted that would allow a covered entity to structure its fundraising programs around the efforts of specific departments, physicians and clinical research efforts and allow access, without authorization, to PHI for those purposes of the covered entity.

2. Fundraising by Business Associates or Institutionally Related Foundations

The Privacy Rule states that in those cases where a covered entity discloses PHI to a business associate or related foundation that is not a part of the covered entity, then the PHI that could be disclosed without authorization is limited to demographic information and dates of service.

Recommendation: The University supports the AAMC position that this restriction creates a serious impediment to the fundraising that is essential for academic health centers and recommends that the Department add the following third exception to 164.514 (f)(l):

(f)(1) Standard: Uses and disclosures for fundraising. A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of section 164.508:

(i) Demographic information relating to an individual;
(ii) Dates of health care provided to an individual; and
(iii) <u>The physician, department, or division of the covered entity from which the individual received treatment.</u>

F. Research

The University appreciates the Secretary's efforts to improve the workability of the Privacy Rule for research, and we offer the following comments in the spirit of further enhancing the Privacy Rule's workability for research institutions while not unduly raising additional patient concerns regarding the use of their PHI in research protocols. The raising of such concerns could create real obstacles to patient participation in vital research.

<u>1. Revocation of research authorization.</u>

Recommendation: If an individual revokes their authorization for use of PHI derived from participation in a research study, there should be provisions that allow the covered entity receiving the information to continue to use it for:

a. Future notification of the individual regarding research findings that may bear upon their own health and well being (e.g., they may have had a research procedure with long term personal health consequences such as the insertion of an experimental form of cardiac pacemaker, for which the right to use research data for future notification needs to be allowed);
b. Maintenance of the scientific integrity of the study and safety of all persons participating in the study. For example, a participant who withdraws may have had an adverse event. Knowledge that an adverse event occurred is important to the protection of the interests of all participants as well as to the validity of the statistical inferences derived from study data. These safety, scientific integrity and human subjects protections-related uses of data should be allowed even if the participant withdraws authorization for use of their research data.
c. If a patient's data has been used in an aggregated data set, the patient's PHI would not need to be extracted from the aggregated data set in those cases where the aggregation of the data renders the patient's individually identifiable information indistinguishable from other data within the set.

2. Accounting for research disclosures.

The University strongly endorses the NPRM recommendation to eliminate the accounting requirements for disclosures made pursuant to patient authorization, including authorization for research purposes. However, continuing to require accounting for all research disclosures made pursuant to a waiver of authorization that has been approved by an IRB will add an additional and unnecessary administrative burden to University IRBs. Since the Privacy Rule affords a waiver of authorization equal weight with the authorization for use and disclosure of information, the exception to accounting should likewise be consistent for both authorization and waiver of authorization. The IRB is already responsible for reviewing the merit of requests for use of PHI without authorization, and those criteria specifically require that the research and confidentiality risks be minimal. Thus, the requirement for accounting of disclosures should also be waived.

The University respectfully disagrees with the proposal of the AAMC to modify the accounting for disclosures provision such that the patient would be provided with a list of all protocols under which the patient's information may have been disclosed pursuant to a waiver of authorization. At major research institutions such as the University of California, that number of possible protocols will number in the hundreds, though in actual practice few, if any, may have accessed the patient's PHI. Providing the patient with a list of potentially hundreds of research protocols could be both shocking and an inaccurate portrayal of the actual probability that the PHI has been used for even a single research protocol.

Recommendation: Eliminate the accounting for all research disclosures made pursuant to a waiver of authorization approved by an IRB.

3. De-identification of Data

In the AAMC's April 11, 2002 comment letter on the Privacy Rule NPRM, the AAMC recommends specific modifications to Section 164.514, the Standard for de-identification of protected health information and implementation specifications. The AAMC believes that the workability of the Privacy Rule for research "hinges upon adoption of a modified de-identification standard for research uses and disclosures." The University strongly endorses the AAMC's position and recommendations.

4. Risk of Redisclosure

Under Section 164.508(c)(l)(vi), an authorization must include a statement about the potential redisclosure of PHI and loss of confidentiality. Inclusion of the language in an authorization could have the unintentional consequence of deterring patient participation in research, particularly when it is unlikely that there would ever be disclosure. In those situations where redisclosure could occur, a project sponsor should be treated like a business associate in order to protect health information.

Recommendation: Eliminate the redisclosure alert from research authorizations in those situations where the IRB approves the redisclosure and a Business Associate Agreement has been entered into by the covered entity and third party sponsor of the research project.

G. Employee Health Records

We believe that modifying the definition of "protected health information" to exclude "employment records held by a covered entity in its role as employer" is a positive step that puts employers who are health care providers on an equal footing with all other employers in connection with employee records. For sound reasons, PHI may be contained in employment records; for example, to accommodate the disability of an employee. An employer who accommodates this disability may have information about the employee's condition and the necessary accommodations that need to be made in the employment record. Those records should not be subject to the Privacy Rule. In addition, the NPRM solicits comments on whether the term "employment records" is clear or needs to be further explained.

Recommendation: Since the definition of "employment record" is one that can vary by institution and industry and in order to increase clarity, the University recommends that the following underlined language be added:

"…employment records held by a covered entity in its role as employer or information used by the employer to take appropriate action as required by other state or federal law relative to an employee's health or well being in the workplace."

Recommendation: A similar change should be made so that employment-related services are not considered "treatment" for purposes of requiring health care providers who are employers to provide a Notice of Privacy Practices in connection with employment-related monitoring or testing as is currently required by section 164.520.

***

The University's individual and institutional providers of health care respect a patient's expectations that the privacy and security of individual health information will be protected. The University is committed to implementing policies and practices that will enable us to reasonably and appropriately protect our patient's privacy while carrying out our mission of care, service, education and research. The University's HIPAA Taskforce has reviewed the NPRM and the impact of the proposed changes on our ability to balance the privacy rights of the University's patients, the patient's expectation that quality care will be delivered in a cost-effective and timely manner, and society's expectation that academic health centers will continue to teach and perform leading edge research.

The University appreciates the opportunity to respond to the NPRM. Should you have any questions regarding the comments provided, please contact Maria Faer, DrPH, Director of HIPAA and Corporate Compliance, University of California Office of the President at 510-987-9262 or maria.faer@ucop.edu.

Sincerely,

William H. Gurtner, Vice President

Cc: AVP Scott Sudduth
University of California HIPAA Taskforce